



Common Logistics Command and Control System

C2PC Logistics Injector Installation Guide

United States Marine Corps

Office of Naval Research

Naval Facilities Engineering Service Center

Marine Corps Systems Command

Sapient Corporation

Georgia Tech Research Institute

DECEMBER 23, 2003

Table of Contents

1. Installation	2
1.1 Installation	2
1.2 IIS Settings Changes	6
1.3 Database Settings	7
Installation Validation	8
3. Secure Access to CLC2S (Optional)	10
Step 1: Installing Security Certificate on CLC2S Server	10
Step 2: Setup the Port Number for HTTPS Access	11
Step 3: Bypass Security Alert	12



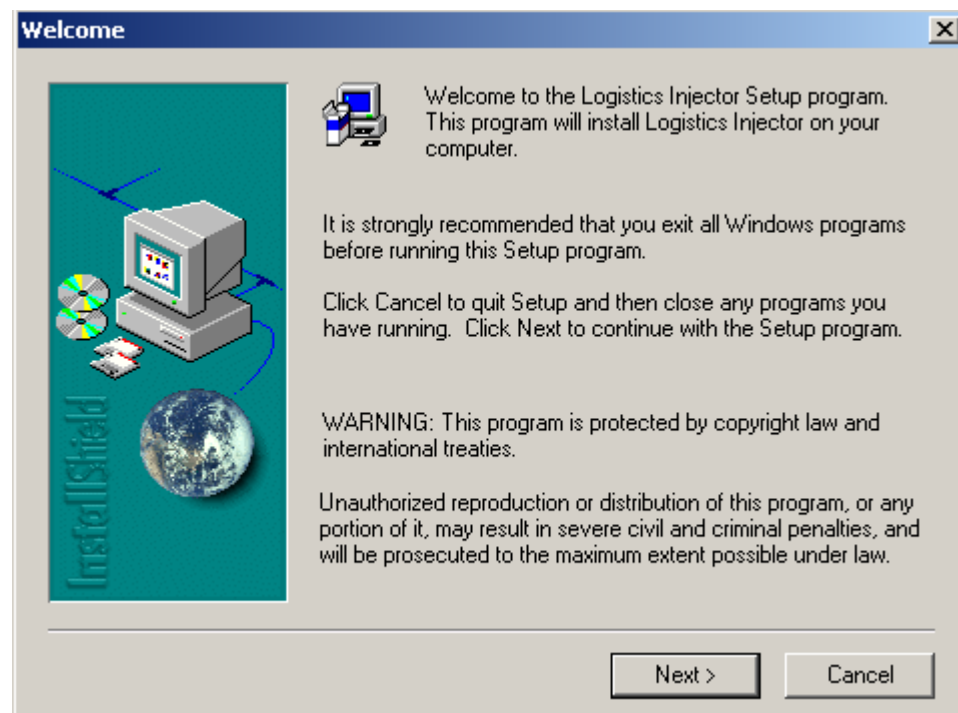
1. Installation

1.1 Installation

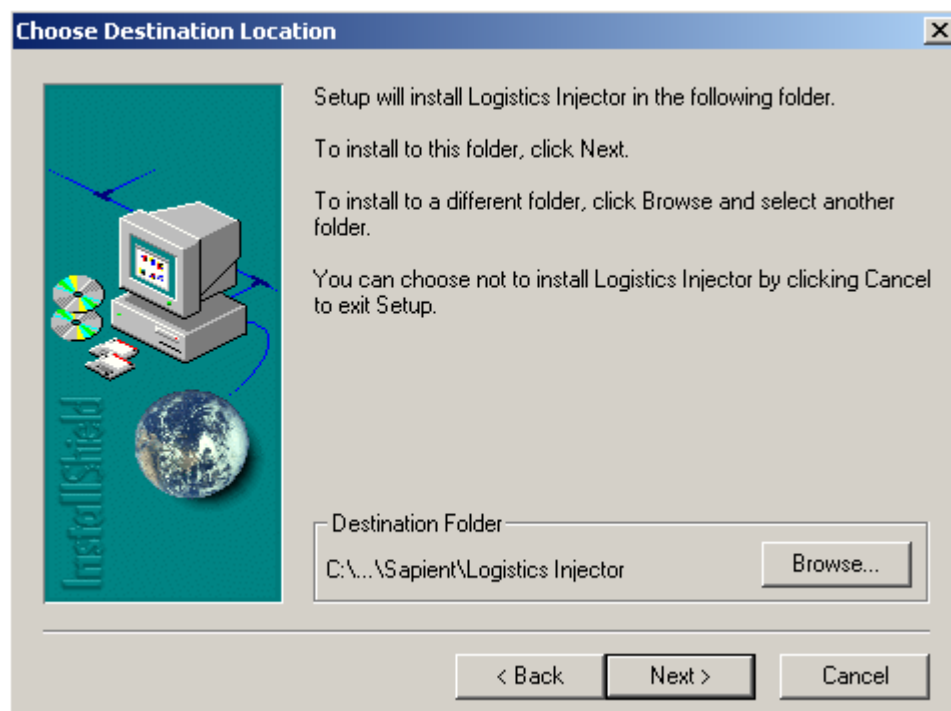
This section describes how to install the Command and Control PC (C2PC) Logistics Injector on a C2PC Client workstation. This guide assumes that you have a working **C2PC client** installation of version **5.8.X**, version **5.9.X** or version **6.0.X** on the machine you are installing the C2PC Logistics Injector. The CLC2S Logistics Injector for C2PC is compatible with Windows 2000 Professional and Server editions as well as Windows XP.

If you do not have a pre-existing C2PC installation, install the C2PC client from the appropriate media and verify that your C2PC client installation works before proceeding further. Setup for secure access is covered at the end of the document.

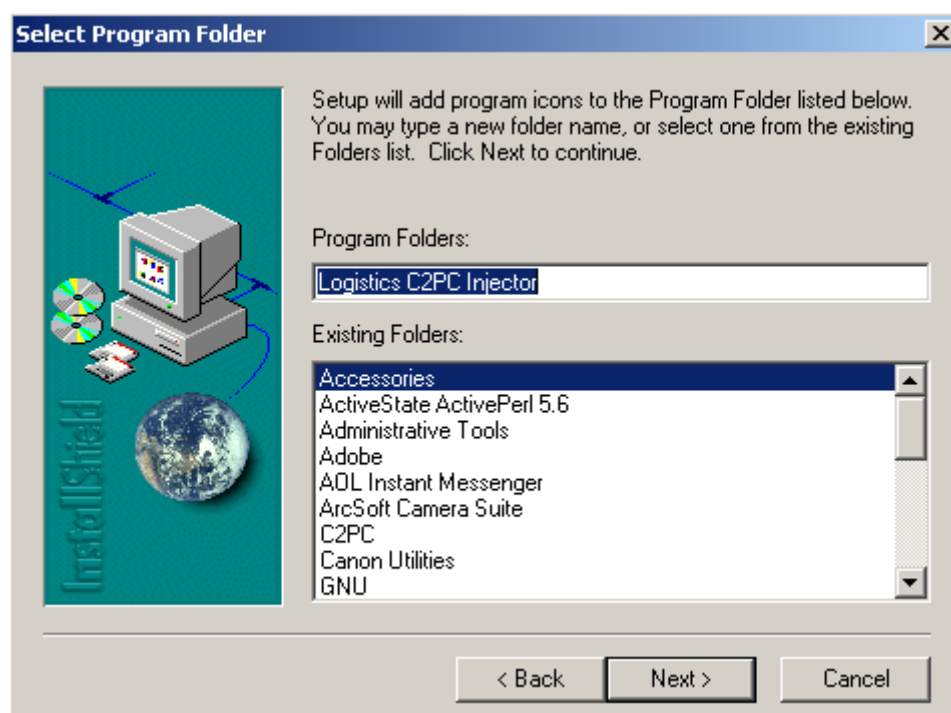
Start the Injector installer by double clicking on the "Setup.exe" file in the C2PC folder of the CLC2S installation media.



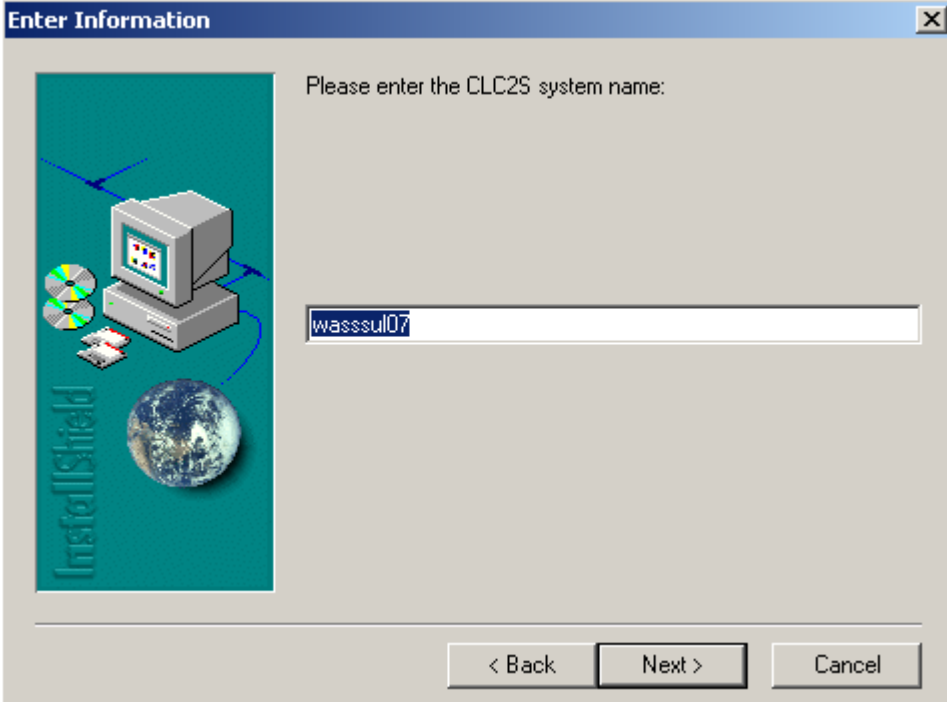
Click the "Next >" button.



Choose the installation location and click the "Next >" button.

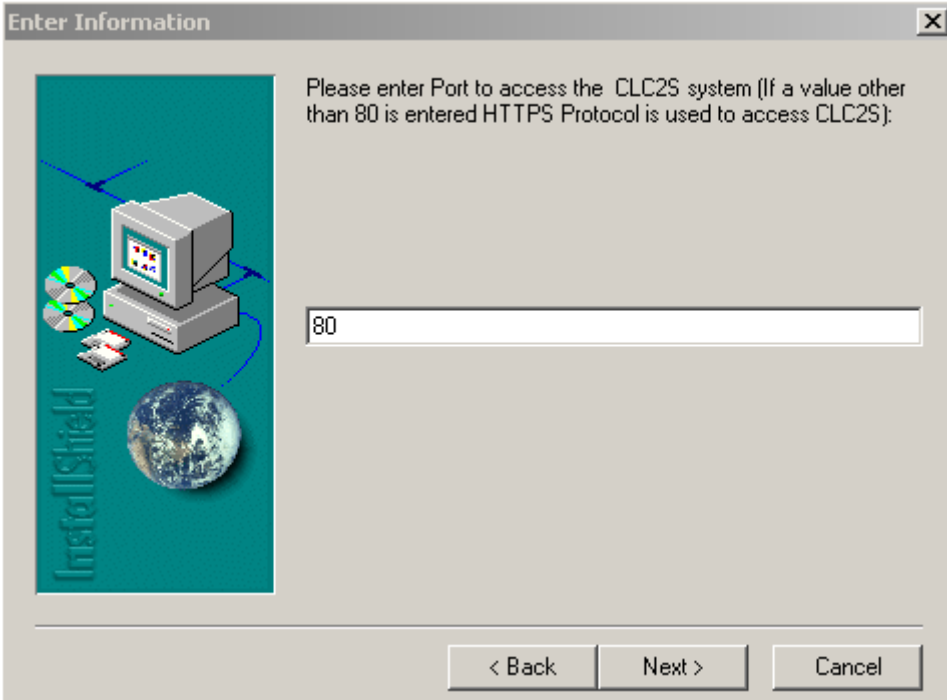


Click the "Next >" button.



The dialog box is titled "Enter Information" and contains a graphic on the left with a computer, CDs, and a globe, with the text "InstallShield" written vertically. The main text reads: "Please enter the CLC2S system name:". Below this is a text input field containing "wassul07". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

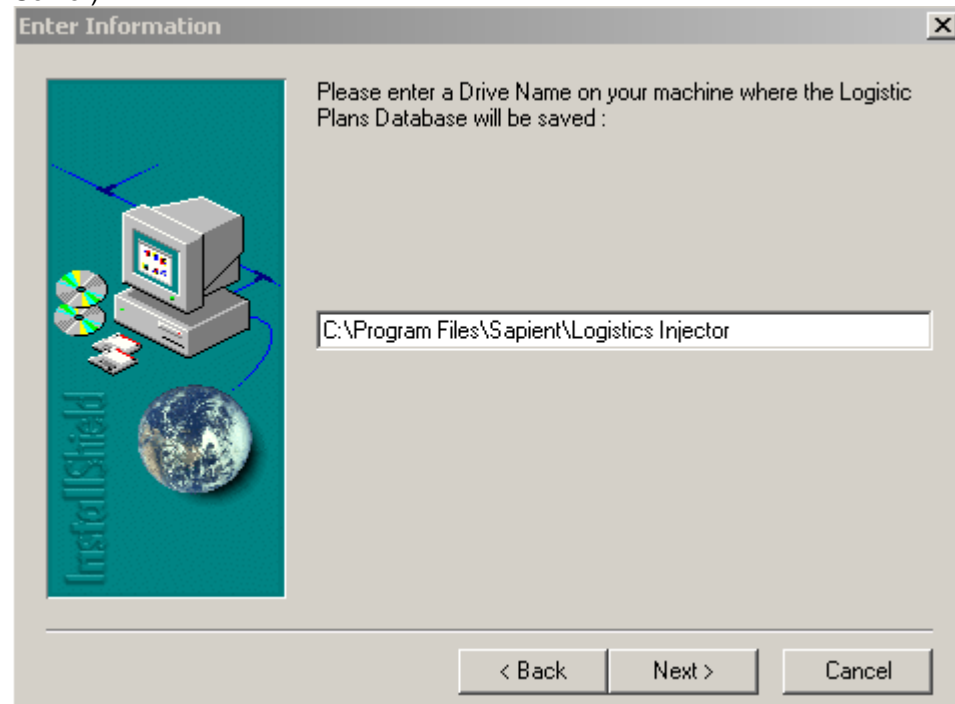
Click the "Next >" button after entering the name of the CLC2S Web Server name that is on the network.



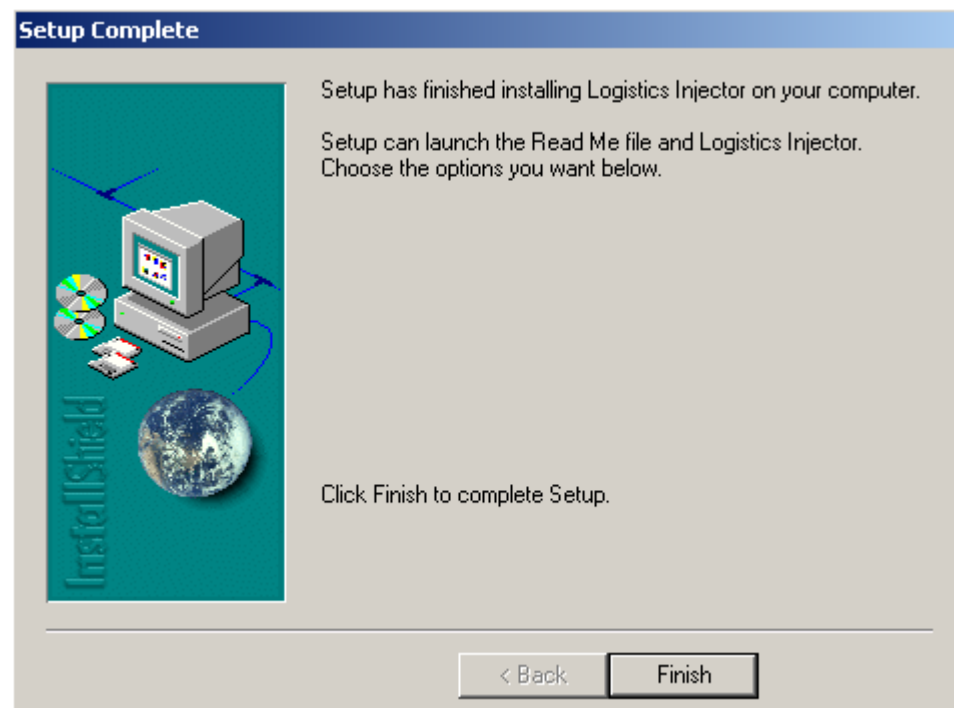
The dialog box is titled "Enter Information" and contains the same graphic as the previous one. The main text reads: "Please enter Port to access the CLC2S system (If a value other than 80 is entered HTTPS Protocol is used to access CLC2S):". Below this is a text input field containing "80". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

Click the "Next >" button after entering the Port used to access the CLC2S system. This is typically 80. If a secure connection is needed to the CLC2S Server then enter the

HTTPS Port Number 443 (Note: A security certificate should be installed on the CLC2S Server)



Click the “Next >” button after entering the Path for the Database to store the Missions created in the Logistics Injector



Click on “Finish”. Your Installation of C2PC Logistics Injector is now complete.

1.2 IIS Settings Changes

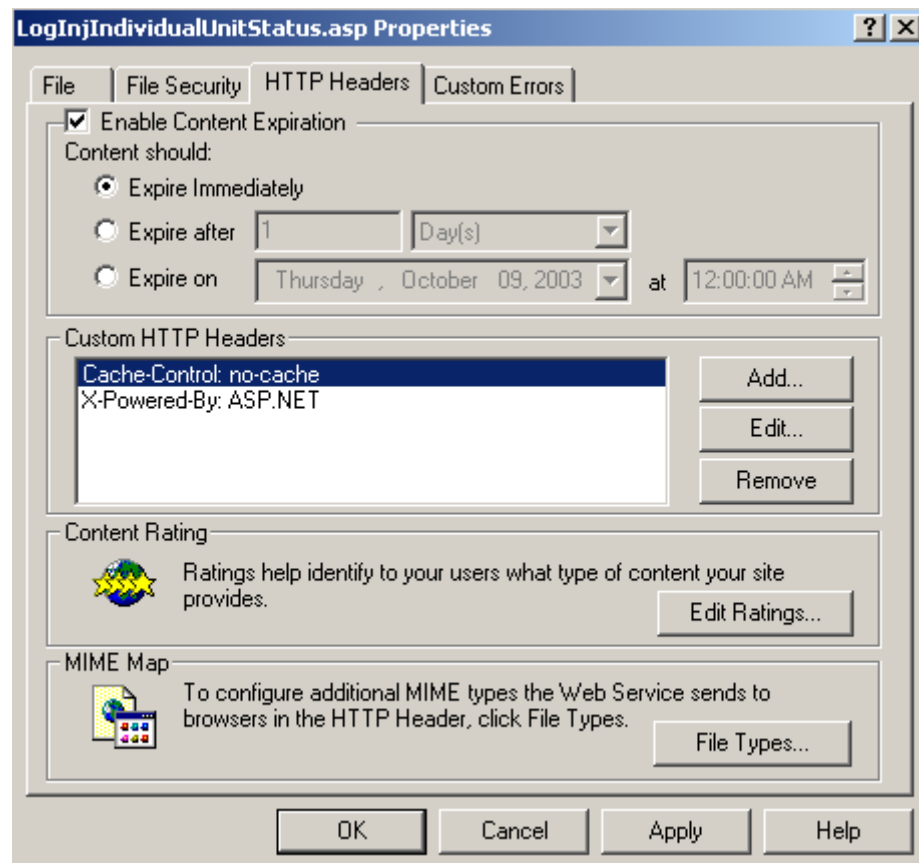
The HTTP Header settings for the following two ASP Pages needs to be changed in IIS

\\SUL\\SUL\\LogisticsInjector\\LogInjIndividualUnitStatus.asp

\\SUL\\SUL\\LogisticsInjector\\LogInjObsUnitStatus.asp

Cache-Control: no-cache

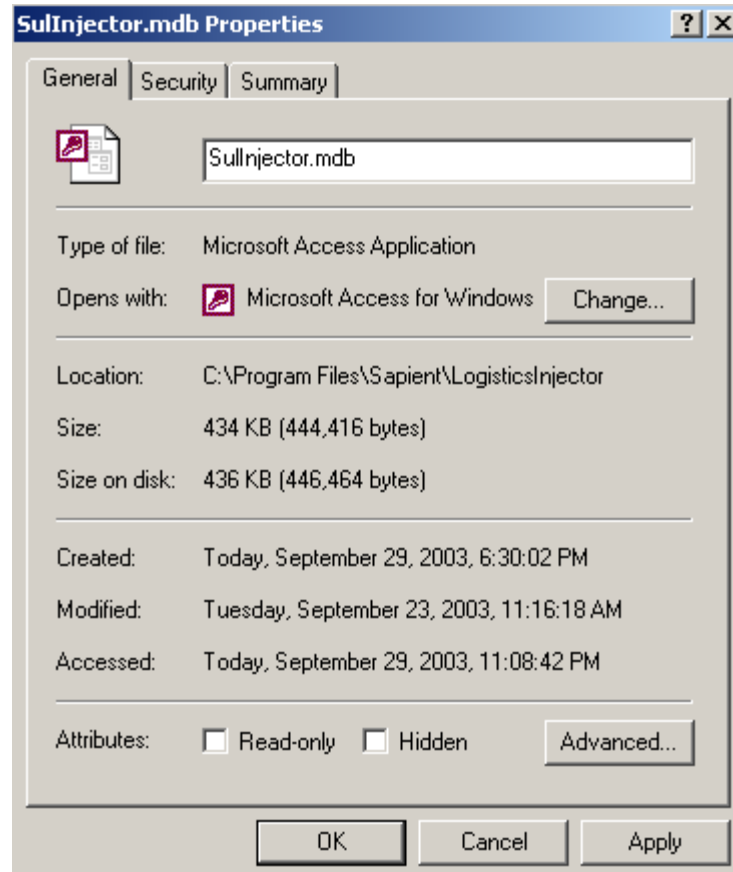
Content: Expire Immediately



1.3 Database Settings

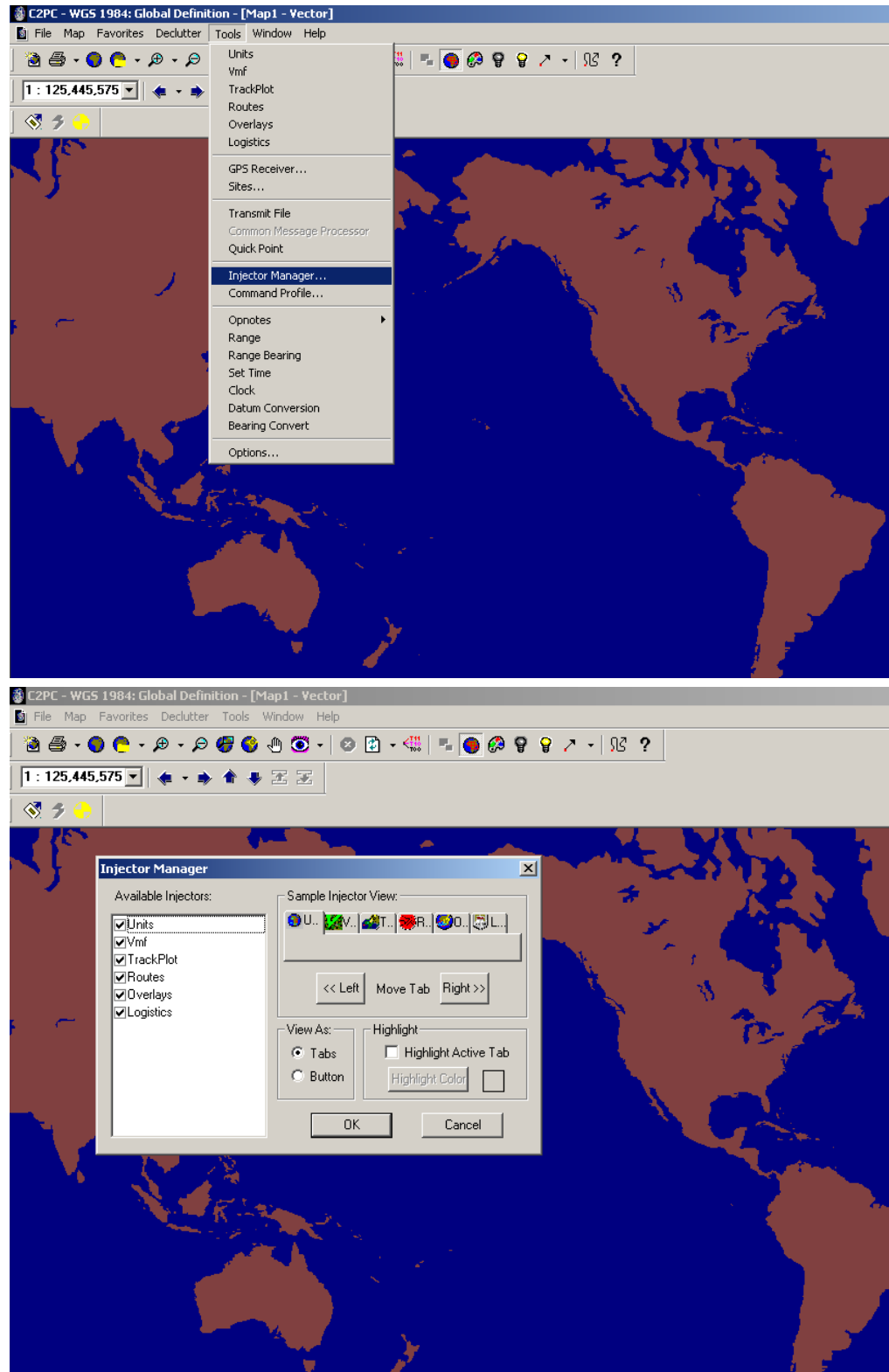
Validate that the database (used for Storing Missions/COAs) installed with the C2PC Logistics Injector is **Writable** (The Read-only setting should be unchecked). It is an MS Access MDB file installed at the following location (unless specified otherwise at the time of install)

C:\Program Files\Sapient\LogisticsInjector\SullInjector.mdb

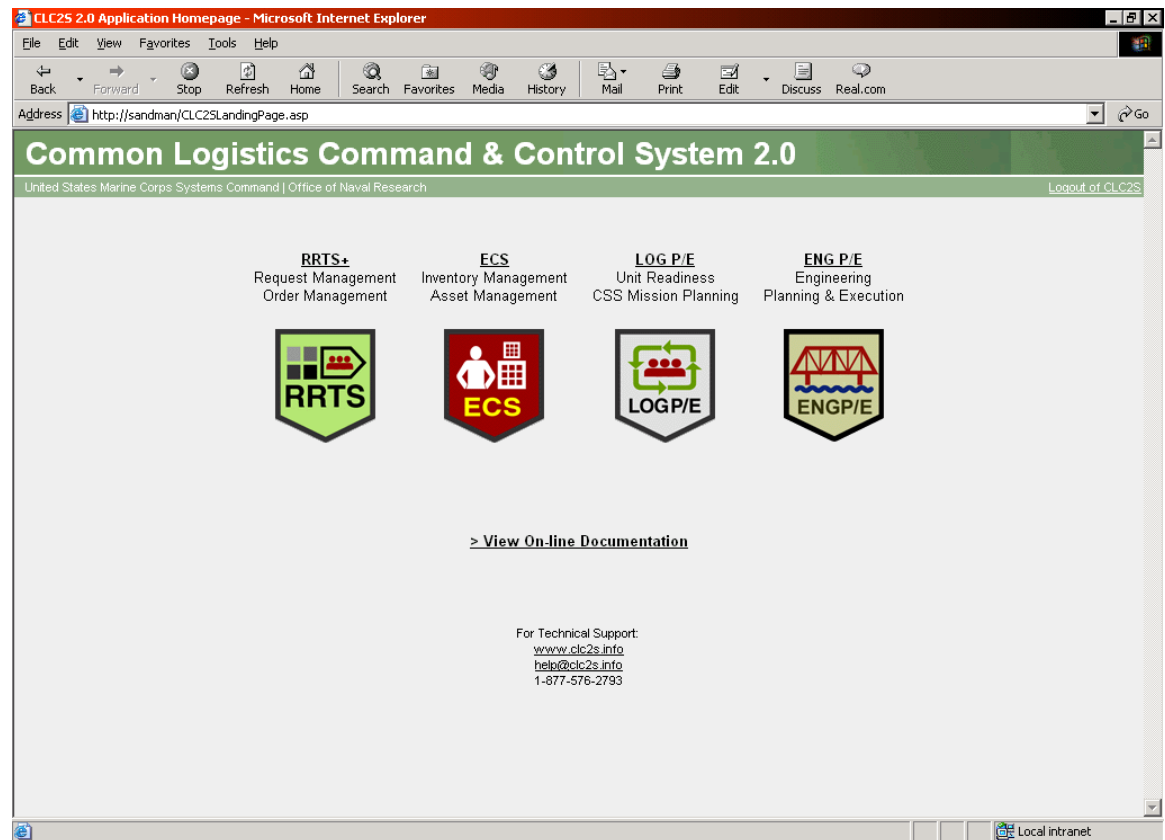


Installation Validation

Validation 1: Open C2PC and validate that the Logistics Injector is selected (“Logistics” should be checked in the Injector Manager)



Validation 2:: Verify that you have CLC2S accessible from your system by opening a browser and navigating to <http://CLC2SServerName/>. (CLC2SServerName should be the name of the Web Server where CLC2S is Installed)



3. Secure Access to CLC2S (Optional)

The C2PC Logistics Injector accesses data from CLC2S via HTTP using the Windows Wininet API. The C2PC Logistics Injector can be setup to access CLC2S via HTTPS (Secure Connection). Setting C2PC Logistics Injector in this configuration is optional.

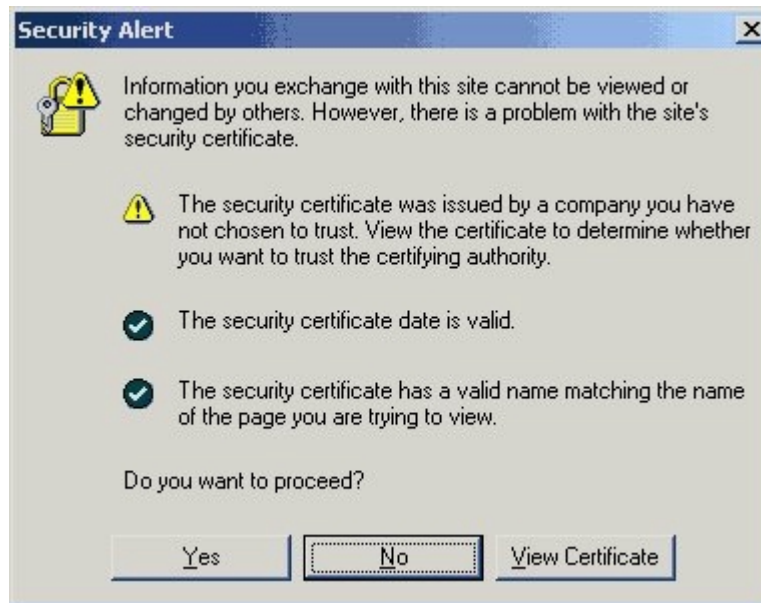
It is a 2-Step Process

Step 1: Installing Security Certificate on CLC2S Server

The CLC2S Server should have a Security Certificate Installed. In order to verify this open a browser and enter <https://CLC2SServerName/>. If the following page is displayed then it implies that a Security Certificate has been installed on the CLC2S Server

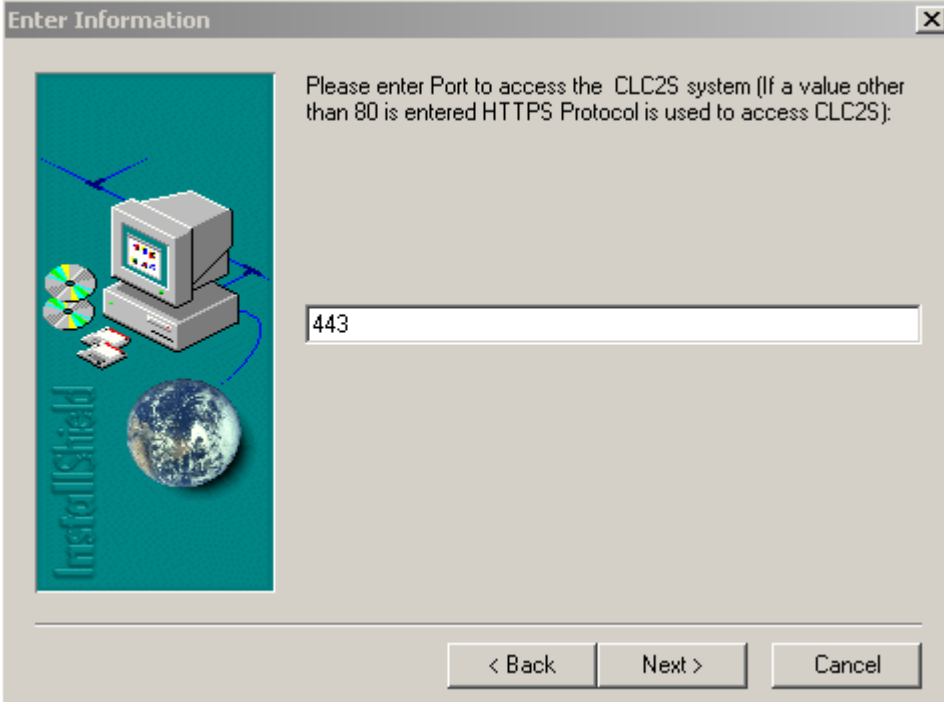


Note: If a Security Alert is displayed on trying to access CLC2S using HTTPS (as displayed in the image below) follow instructions in "Step 3" to bypass the Security Alert.



Step 2: Setup the Port Number for HTTPS Access


The Port Number for HTTPS for CLC2S access should be specified during the installation of the C2PC Logistics Injector (See Section 1 of this document). If a value other than 80 is entered then HTTPS Protocol is used to access CLC2S (The default port for HTTPS access is 443)



The "Enter Information" dialog box has a title bar with a close button. On the left is a graphic with a computer, CDs, a globe, and the text "InstallShield". The main text reads: "Please enter Port to access the CLC2S system (If a value other than 80 is entered HTTPS Protocol is used to access CLC2S):". Below this is a text input field containing "443". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

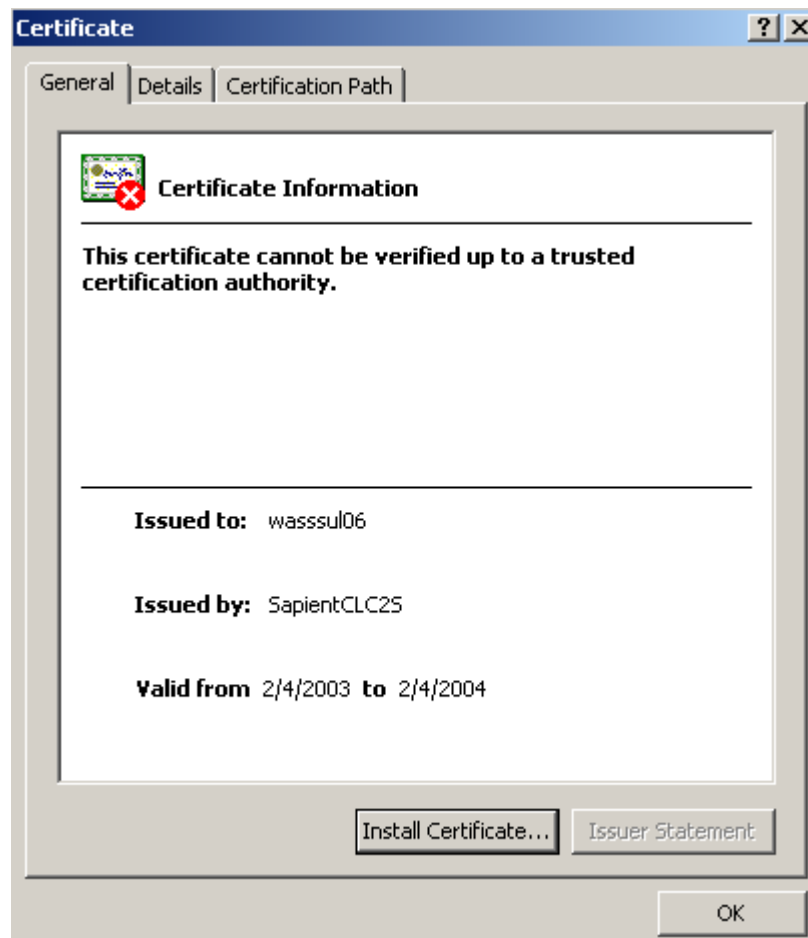
Step 3: Bypass Security Alert

(Note: Only needed if Security Alert is displayed in Step 1)

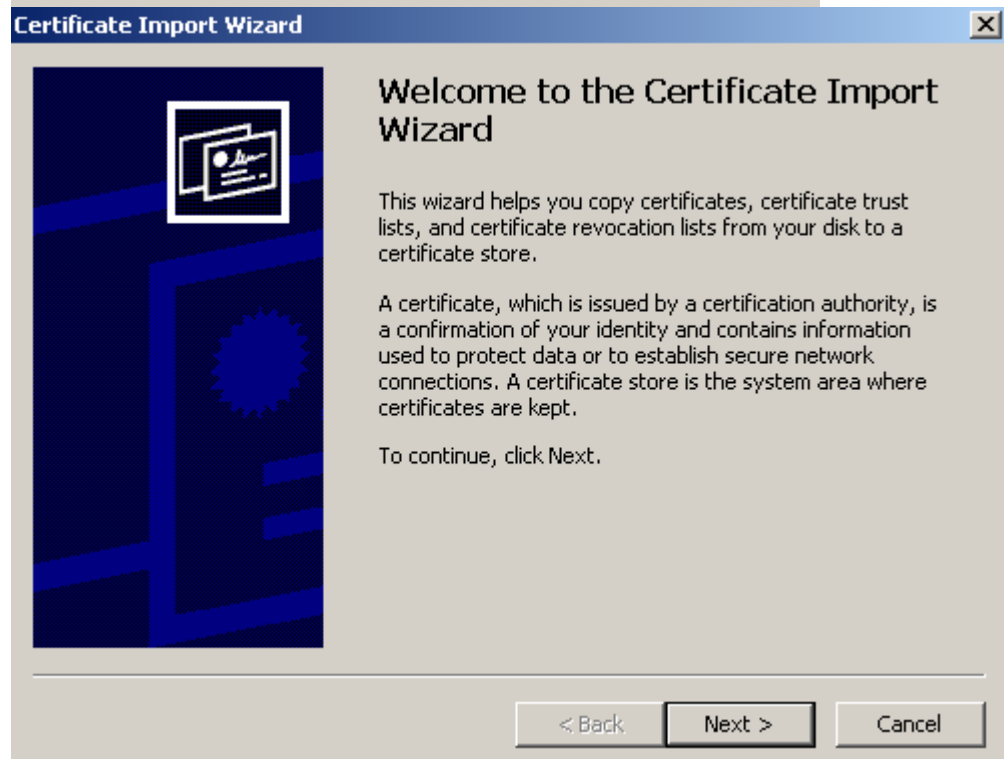


The "Security Alert" dialog box has a title bar with a close button. It features a yellow warning icon. The main text states: "Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate." Below this are three items: a warning icon with the text "The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.", a green checkmark with "The security certificate date is valid.", and another green checkmark with "The security certificate matches the name of the page you are trying to view." The question "Do you want to proceed?" is followed by three buttons: "Yes", "No" (which is selected), and "View Certificate".

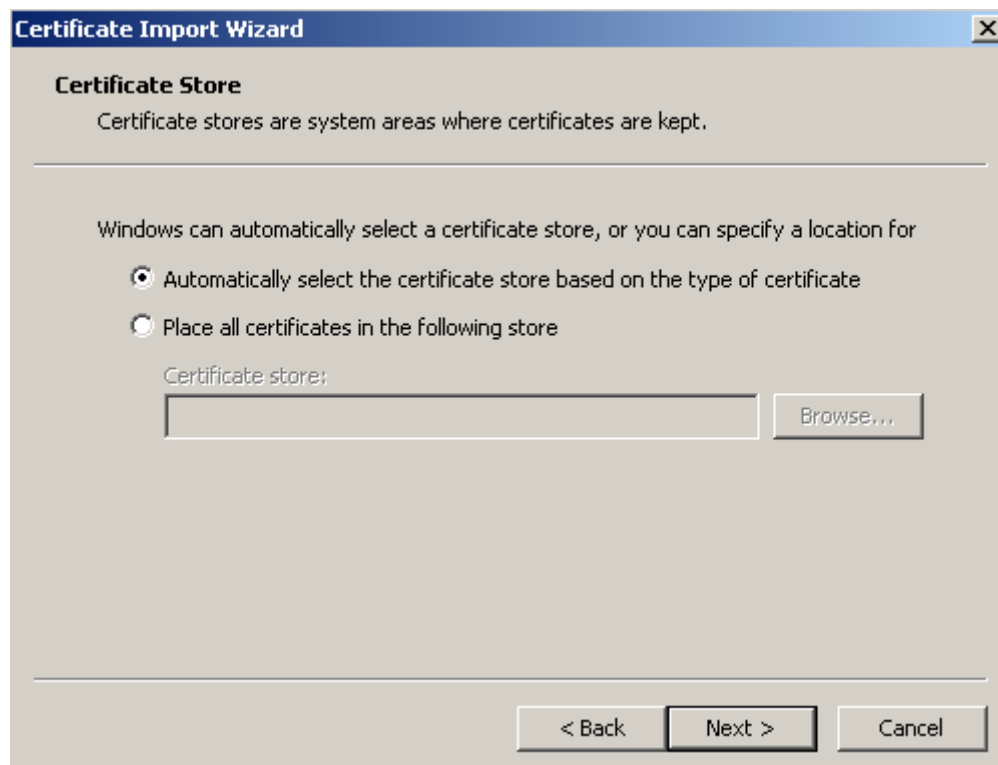
In order to bypass the "Security Alert" (seen above) when logging into <https://CLC2SServerName> click on "View Certificate"



Select "Install Certificate":



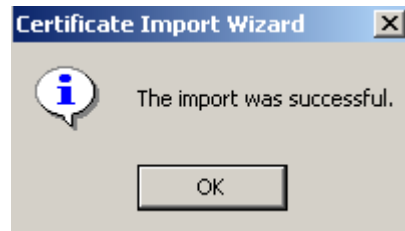
Click on "Next >" on the "Certificate Import Wizard" screen



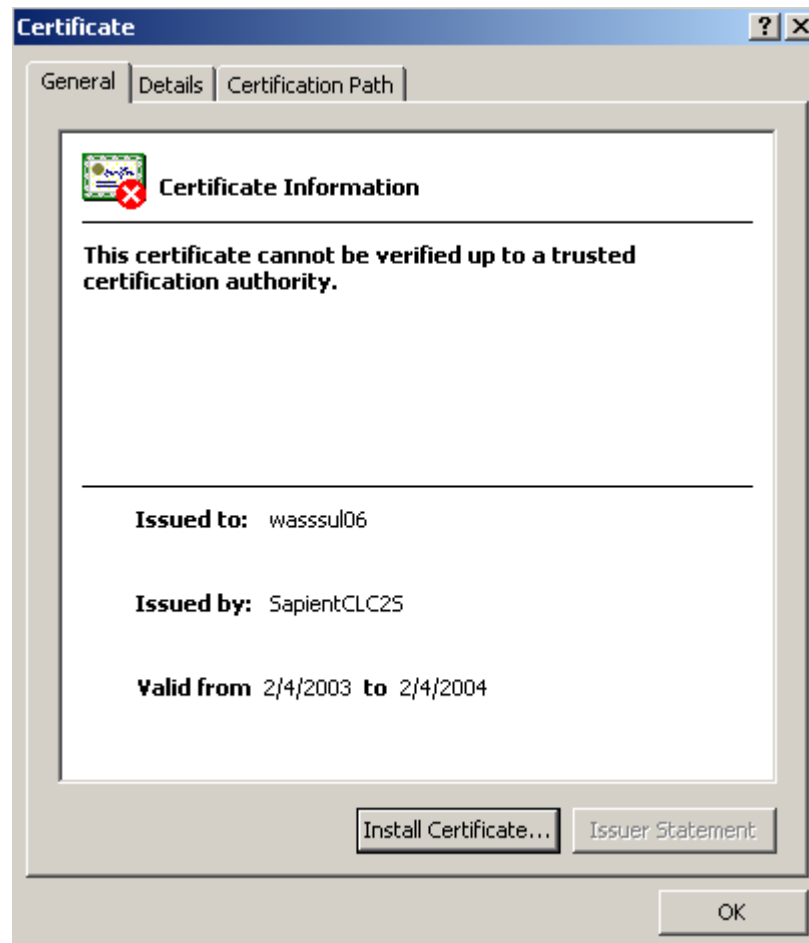
Ensure the selected option is "Automatically select the certificate store based on the type of certificate" and then click "Next >"



Click on "Finish" on the last import screen (Click on "Yes" to store the Root Certificate if prompted)



If import was successful then you should be prompted to click "OK" on the dialog that says "The import was successful."



Click on "OK" to close the Certificate window

Note: Now, The Security Alert should not be displayed when accessing
<https://CLC2SServerName> using a browser

